Consorzio di Bonifica Della Media Pianura Bergamasca Via Gritti 21/25, 24125 BERGAMO
Tel. +39 035 4222.111
info@cbbg.it / info@pec.cbbg.it

Modello Organizzativo e di gestione
Decreto Legislativo 8 giugno 2001, n. 231

Parte Speciale E REATI INFORMATICI

Esaminato ed adottato con deliberazione n. 022 del Consiglio di Amministrazione del

25 maggio 2021

IL PRESIDENTE	IL SEGRETARIO
F.to (Franco Gatti)	F.to (Mario Reduzzi)

Sommario

1.Premessa

L'art. 24 bis intitolato "*Delitti informatici e trattamento illecito dei dati*" punisce con sanzioni pecuniarie e in alcuni casi interdittive di varia natura applicate direttamente a carico dell'Ente la violazione di alcune norme del vigente Codice penale, che prevedono ipotesi strettamente legate ad aspetti rientranti nella disciplina della privacy, intesa non solo quale tutela dei dati personali, ma anche di tutti gli altri dati rinvenibili in un sistema informatico.

Appare evidente che si tratta di ipotesi delittuose che possono essere poste in essere laddove sia carente ovvero non dimostrabile una corretta ed adeguata tutela dei dati personali trattati in ambito aziendale.

Il D. Lgs. n. 231/2001 ha, quindi, ricompreso nel novero dei reati cd. presupposto fattispecie strettamente legate ai profili della protezione dei dati in ambito aziendale, configurando un ulteriore profilo di punibilità a carico dell'ente con elevate sanzioni pecuniarie e, nelle ipotesi delittuose più gravi, anche interdittive dell'attività con confisca del profitto e pubblicazione della sentenza.

Quanto ai delitti informatici nell'ambito dell'emergenza sanitaria da Covid-19, gli enti e le imprese si devono confrontare con una selva di nuove norme volte a fornire indicazioni e prescrizioni su come riorganizzare gli spazi di lavoro, le modalità di accesso agli stessi, i rapporti interpersonali e come gestire eventuali casi di positività al COVID-19 all'interno dell'azienda, il tutto nel rispetto delle regole a tutela della privacy dei lavoratori.

In particolare, il ricorso allo strumento dello smart working ha creato nuovi rischi, tra cui quello di incorrere in illecita raccolta di dati dei lavoratori o quello che il telelavoro possa costituire, anche involontariamente, occasione per commettere uno o più dei reati informatici presupposti dall'art. 24-bis D.Lgs. 231/2001 (accesso abusivo ad un sistema informatico o telematico; detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico; Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; danneggiamento di sistemi informatici o telematici di pubblica utilità).

Con riguardo al trattamento illecito di dati collegati alla emergenza Covid, il problema si pone in relazione alla verifica della temperatura corporea dei lavoratori e alle autodichiarazioni attestanti la non provenienza dalle zone a rischio epidemiologico e l'assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al Covid-19: il trattamento di tali dati va, pertanto, adeguatamente organizzato in contesto privacy, prevedendo modalità di raccolta che assicurino riservatezza ai soggetti interessati, conservazione dei dati, con rigorosa applicazione del principio di minimizzazione (raccolta e conservazione dei dati effettivamente necessari).

Il mancato rispetto delle regole poste a tutela della riservatezza dei dati personali dei lavoratori o di altri soggetti che entrano in contatto con l'ente potrebbe condurre ad una doppia responsabilità: per la violazione delle norme sulla privacy e per la violazione dell'art. 24-bis D.Lgs. n. 231/01 con sanzione fino 400 quote.

2.Delitti informatici e trattamento illecito di dati

Art. 615 ter – "Accesso abusivo ad un sistema informatico o telematico"*: "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro*

la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) *se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;*
2) *se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;*
3) *se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.*

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio."

Art. 617 quater – "Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche": "*Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.*

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia, si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) *in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;*
2) *da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;*
3) *da chi esercita anche abusivamente la professione di investigatore privato."*

Art. 617 quinquies – "Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche"*:* "*Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.*

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617- quater."

Art. 635 bis – "Danneggiamento di informazioni, dati e programmi informatici": *"Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni."*

Art. 635 ter – "Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità"*: "Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.*

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata."

Art. 635 quater – "Danneggiamento di sistemi informatici o telematici": *"Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.*

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata."

Art. 635 quinquies – "Danneggiamento di sistemi informatici o telematici di pubblica utilità": "*Se il fatto di cui all'articolo 635 quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.*

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata."

Art. 615 quater – "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici": "*Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.*

La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater."

Art. 615 quinquies – "Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico": "*Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni con la multa sino a euro 10.329."*

Art. 491 bis – "Documenti informatici": "*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso*

concernenti rispettivamente gli atti pubblici."

Art. 640 quinquies – "Frode informatica del soggetto che presta servizi di certificazione di firma elettronica": "*Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro*."

Art. 1, comma 11 D. L. n. 105/2019 – "Perimetro di sicurezza nazionale cibernetica": "11. *Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni*".

3. Le sanzioni previste in relazione all'art. 24 bis del D. Lgs. n. 231/2001

Si riporta di seguito una tabella riepilogativa delle sanzioni previste con riferimento ai reati contemplati dall'art. 24 bis del D. Lgs. n. 231/2001 a carico del Consorzio qualora, per effetto della commissione dei reati indicati al precedente paragrafo 2 da parte dei Soggetti Apicali e/o dei Soggetti Sottoposti, derivi allo stesso un interesse o un vantaggio.

Reato	Sanzione pecuniaria	Sanzione interdittiva
Art. 615 ter – "Accesso abusivo ad un sistema informatico o telematico"	Da 100 a 500 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca della autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi
Art. 617 quater – "Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche"	Da 100 a 500 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca della autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi
Art. 617 quinquies – "Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche"	Da 100 a 500 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca della autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi
Art. 635 bis – "Danneggiamento di informazioni, dati e programmi	Da 100 a 500 quote	Interdizione dall'esercizio dell'attività;

informatici”		sospensione o revoca della autorizzazioni, licenze o concessioni funzionali alla commissione dell’illecito; divieto di pubblicizzare beni o servizi
Art. 635 ter – “Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità”	Da 100 a 500 quote	Interdizione dall’esercizio dell’attività; sospensione o revoca della autorizzazioni, licenze o concessioni funzionali alla commissione dell’illecito; divieto di pubblicizzare beni o servizi
Art. 635 quater – “Danneggiamento di sistemi informatici o telematici”	Da 100 a 500 quote	Interdizione dall’esercizio dell’attività; sospensione o revoca della autorizzazioni, licenze o concessioni funzionali alla commissione dell’illecito; divieto di pubblicizzare beni o servizi
Art. 635 quinquies – “Danneggiamento di sistemi informatici o telematici di pubblica utilità”	Da 100 a 500 quote	Interdizione dall’esercizio dell’attività; sospensione o revoca della autorizzazioni, licenze o concessioni funzionali alla commissione dell’illecito; divieto di pubblicizzare beni o servizi
Art. 615 quater – “Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici”	Fino a 300 quote	sospensione o revoca della autorizzazioni, licenze o concessioni funzionali alla commissione dell’illecito; divieto di pubblicizzare beni o servizi
Art. 615 quinquies – “Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	Fino a 300 quote	sospensione o revoca della autorizzazioni, licenze o concessioni funzionali alla commissione dell’illecito; divieto di pubblicizzare beni o servizi
Art. 491 bis – “Documenti informatici	Fino a 400 quote	il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già

		concessi; il divieto di pubblicizzare beni o servizi
Art. 640 quinquies – "Frode informatica del soggetto che presta servizi di certificazione di firma elettronica	Fino a 400 quote	il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi
Art. 1, comma 11 D. L. n. 105/2019 – "Perimetro di sicurezza nazionale cibernetica"	Fino a 400 quote	il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi

4. PROTOCOLLO DI COMPORTAMENTO E DI PREVENZIONE

4.1. Norme di comportamento

È imposto il divieto nei confronti del CDA, della DG, dei dipendenti e dei collaboratori esterni del Consorzio di porre in essere, collaborare o dare causa alla realizzazione di comportamenti e/o fatti che – considerati individualmente o collettivamente – integrino, direttamente o indirettamente, le fattispecie di reato informatico previste dal D.lgs. n. 231/2001 sia nella forma consumata che nella forma tentata.

In particolare, è fatto espresso divieto di:

- tenere qualunque comportamento che, sebbene non appaia idoneo a costituire di per sé una o più fattispecie di reato informatico, possa potenzialmente realizzarlo;
- utilizzare informazioni, applicazioni ed apparecchiature informatiche per ragioni diverse rispetto a quelle lavorative;
- cedere o prestare a altri soggetti l'utilizzo delle apparecchiature informatiche in assenza di alcuna esigenza aziendale giustificata;
- diffondere, utilizzare, copiare, trasferire, inoltrare *files* e/o documenti informatici e/o qualunque altra documentazione riservata nonché relativa all'attività del Consorzio salvo il caso in cui ciò si renda necessario per il conseguimento dell'oggetto sociale;
- lasciare non custodito il proprio PC senza averlo reso non accessibile agli altri operatori;
- utilizzare le credenziali di accesso al sistema informatico di altri soggetti, salvo previo loro espresso consenso e solo per ragioni di carattere lavorativo e mai personale;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- cancellare e/o alterare e/o manomettere e/o distruggere informazioni, dati o documenti informatici;
- detenere e/o diffondere e/o utilizzare abusivamente codici, parole chiave, o altri mezzi idonei all'accesso ad un sistema informatico o telematico al fine di acquisire informazioni riservate di concorrenti;
- alterare, cancellare, distruggere, falsificare documenti informatici ricevuti e/o disponibili sul server relativi all'attività gestionale dell'Ente;
- accedere abusivamente a sistemi interbancari;
- accedere abusivamente a sistemi dell'Ente protetti da misure di sicurezza al fine di attivare servizi non richiesti dalla clientela;
- detenere e utilizzare le credenziali di accesso alle caselle di posta e – mail dei dipendenti salvo che ciò si renda necessario al fine di acquisire informazioni relative all'attività svolta dal Consorzio e solo previo consenso del soggetto interessato;
- diffondere abusivamente numeri seriali di telefoni cellulari;
- danneggiare informazioni/dati aziendali/programmi aziendali infrastrutture tecnologiche/sistemi di conservazione dei documenti di soggetti concorrenti;
- danneggiare, distruggere, manomettere documenti probatori registrati presso gli enti pubblici o informazioni, dati e programmi informatici in uso alla PA;
- impedire o interrompere una comunicazione al fine di evitare che un concorrente trasmetta dati e/o l'offerta

per la partecipazione di una gara;

- installare apparecchiature finalizzate ad intercettare ed impedire informazioni informatiche;
- non divulgare informazioni e/o dati e/o documenti riferiti a terzi e/o all'Ente verso l'esterno.

A tale fine, è fatto obbligo al CDA, alla DG, ai dipendenti ed ai collaboratori esterni nei limiti di quanto previsto negli accordi commerciali sottoscritti con il Consorzio:

1) rispettare le regole di comportamento e i valori espressi nel Codice Etico dell'Ente;
2) comunicare all'OdV e/o al proprio Responsabile qualunque anomalia e/o comportamento sospetto di cui si è venuti a conoscenza nell'esercizio della propria attività lavorativa;
3) segnalare tempestivamente e senza indugio ogni anomalia e/o malfunzionamento e/o inoperatività riferita ai sistemi o programmi informatici al Responsabile dell'area informatica;
4) non accedere a sistemi informatici senza il consenso della persona autorizzata;
5) non accedere e/o utilizzare i sistemi o programmi informatici per usi diversi rispetto a quelli per i quali sono stati destinati e al fine di arrecare un danno a terzi o a imprese concorrenti.

4.2. Struttura

La Struttura del Sistema Informatico dell'Ente è suddivisa in:

- **HARDWARE (HW)** a cui appartengono i PC Client (desktop, Notebook, Tablet), i Server, le reti locali LAN (Local Area Network), stampanti, Reti di comunicazione, Supporti di memorizzazione;
- **SOFTWARE (SW)** di base a cui appartengono i sistemi operativi, i software per lo sviluppo di applicazioni e i SW applicativi a cui appartengono i software acquistati da terze parti o sviluppati all'interno dell'Ente ed utilizzati dagli utenti per gestire determinati processi aziendali.

4.2.1. Architettura rete aziendale

STRUTTURA HARDWARE

La rete interna dell'Ente è protetta attraverso un *firewall perimetrale* che consente di discriminare l'accesso a internet esterno.

L'accesso alla rete internet dagli utenti è consentito solo per l'esercizio dell'attività lavorativa.

Nei locali del Consorzio è presente una rete *Wireless Aziendale* a cui possono accedere solo gli utenti espressamente autorizzati dal Responsabile dell'area informatica previa indicazione della DG: solo il Responsabile dell'area informatica è a conoscenza della chiave di ingresso alla rete *Wireless*.

Non è consentito l'accesso alla rete Wireless "Aziendale" mediante l'uso di apparecchi personali.

Esiste una rete Wireless per gli ospiti (Guest) alla quale e' permesso l'accesso da parte degli ospiti del Consorzio senza alcuna area di interazione con la rete Aziendale

La configurazione base dei PC e del Server e la loro caratteristica tipologia di connessione è conservata presso il Responsabile dell'area informatica il quale provvede al suo aggiornamento.

La sala server è collocata al piano terra ed è dotata di controllo degli accessi tramite serratura e l'accesso è consentito solo alla DG e al Responsabile dell'area informatica.

Sono altresì presenti gruppi di continuità distribuiti su distinte linee di alimentazione e configurati per garantire

la continuita' delle operazioni e lo *shutdown ordinato* automatico dei sistemi.

La variazione delle configurazioni base dei PC e del Server sono legate esclusivamente alla sostituzione di un componente HW difettoso e obsoleto:

- sostituzione PC (Desktop e Notebook): obsolescenza o rottura;
- spostamenti di postazione per gli utenti: solo in presenza di un giustificato motivo oggettivo o soggettivo e previa determinazione della DG e del Responsabile dell'area informatica;
- sostituzione HW e alimentatore: solo in caso di rottura;
- sostituzione scheda di rete: solo in presenza di ragioni obbiettive e previa determinazione della DG e del Responsabile dell'area informatica.

Le attività di assistenza e manutenzione HW sono valutate tenuto conto della singola situazione oggettiva a cui seguono le dovute misure scelte dal Responsabile dell'area informatica previa consultazione con la DG.

STRUTTURA SOFTWARE

I PC dell'Ente sono in possesso della configurazione SW base decisa, conservata ed aggiornata dal Responsabile dell'area informatica.

L'installazione di qualunque software è di competenza del Responsabile dell'area informatica previo concerto con la DG. Gli utenti non possono installare software – anche gratuiti – né installare dispositivi di memorizzazione, comunicazione o di altra natura (quali, a titolo esemplificativo ma non esaustivo, modem e masterizzatori).

Le azioni di variazione della configurazione base dei SW presenti sui PC e Server sono aggiornamenti del SW e l'installazione di patch di sicurezza (correzioni del SW).

Ogni PC è dotato di procedure di controllo per l'installazione di software sui sistemi operativi e di programmi di protezione da attacchi esterni tramite *antivirus* e filtro in uscita tramite *proxy*.

Qualora il software antivirus rilevi la presenza di un virus nel sistema, l'utente interessato dovrà immediatamente sospendere ogni attività in corso senza spegnere il PC e segnalare l'accaduto al Responsabile dell'area informatica o, in caso di assenza del Responsabile, ad ogni altro operatore disponibile nell'ufficio informatico dell'Ente. Ogni dispositivo esterno dovrà essere sottoposto al controllo antivirus prima di essere utilizzato e qualora venga rilevato un virus, il dispositivo dovrà essere consegnato al Responsabile dell'area informatica che effettuerà le opportune verifiche. Tutti i file contenenti software o eseguibili dovranno essere controllati e contrassegnati come esenti da virus prima della consegna a terzi

GESTIONE DEGLI UTENTI INFORMATICI

La sicurezza all'accesso delle informazioni è garantita dall'autenticazione: ogni utente possiede ID e PSW che gli viene attribuito previa disposizione della DG.

Ogni utente deve essere associato ad un solo profilo abilitativo in relazione al ruolo aziendale che ricopre. In caso di trasferimento o di modifica dell'attività deve essergli attribuito un profilo abilitativo corrispondente al nuovo ruolo assegnato.

La richiesta e la modifica di credenziali di accesso o autenticazione è di esclusiva competenza della DG il quale individua l'ambito di "*operatività informatica*" di ciascun dipendente o collaboratore e lo comunica al Responsabile dell'area informatica il quale provvederà a rendere disponibili all'utente solo i servizi informatici necessari per lo svolgimento della sua attività lavorativa.

Al termine del rapporto di lavoro o della collaborazione le credenziali di accesso o autenticazione in uso al lavoratore verranno, previa richiesta della DG al Responsabile dell'area informatica, disattivate il giorno stesso

della cessazione del rapporto o della collaborazione.

La PSW possiede una validità di 90 giorni e deve possedere almeno 8 caratteri alfanumerici e non deve contenere riferimenti agevolmente riconducibili all'utente; ogni 3 mesi l'utente deve procedere alla modifica della PSW che non potrà essere uguale alle due precedenti utilizzate. La PSW non dovrà essere annotata su documenti cartacei né digitali e non potrà essere uguale a quella utilizzata per accedere ad altri strumenti elettronici o servizi informatici dell'Ente.

Gli utenti non dovranno divulgare i propri ID e PSW né renderli noti all'interno dell'Ente, salvo per comprovate esigenze aziendali e previa determinazione della DG ovvero previa richiesta del Responsabile dell'area informatica qualora ciò si renda necessario per la sistemazione o aggiornamento del PC o del software; in tale caso, il Responsabile dell'area informatica dovrà darne comunicazione all'utente e indicare le ragioni per cui è necessario l'intervento. Gli utenti dovranno registrare il giorno e l'ora in cui è avvenuto l'accesso autorizzato degli altri utenti ed indicare le ragioni aziendali per cui si è ritenuto necessario tale accesso.

Ogni PC è dotato di misure di protezione al fine di negarne l'uso nell'ipotesi in cui l'utente, per ragioni lavorative, deve allontanarsi dalla sua postazione. Ogni PC è dotato di manualità manuale di blocco (CTRL + A LT + CANC) che l'utente dovrà azionare in caso di inutilizzo temporaneo. Ogni PC è altresì dotato di screen saver il quale entra in funzione trascorsi 5 minuti di operatività inattivita' (eccezion fatta per la postazione in reception che ha un time out di 20 min) e la ripresa della sessione di lavoro richiede l'inserimento della chiave di sicurezza. In ogni caso, nessun lavoratore o collaboratore potrà lasciare incustodito o accessibile il proprio PC mentre è in corso una sessione di lavoro. Gli utenti hanno l'obbligo di spegnere il PC prima di lasciare l'ufficio.

Anche l'accesso alle Banche dati dell'Ente avviene tramite un processo di autenticazione. Ogni utente ha l'obbligo di conservare con cura l'ID e la PSW e non divulgarli.

La gestione della tracciatura delle azioni degli utenti è di competenza del Responsabile dell'area informatica.

Gli utenti che usufruiscono del servizio di posta elettronica e della rete internet per l'espletamento della propria attività lavorativa sono stati adeguatamente informati sulle modalità di utilizzo dei suddetti strumenti.

Le credenziali di accesso agli account di posta elettronica di ciascun utente corrispondono a quelle di accesso al sistema informatico. La DG può assegnare account di posta elettronica con credenziali differenti qualora lo ritenga necessario per ragioni di sicurezza. La casella di posta elettronica non può essere utilizzata per ragioni estranee al rapporto di lavoro. E' vietato l'utilizzo della casella di posta per motivi personali.

In particolare, è vietato:

- l'invio e il ricevimento di messaggi personali o la partecipazione a dibattiti, chat, aste on line, forum, concorsi;
- esprimere opinioni e commenti discriminatori;
- non divulgare notizie o informazioni riservate la cui divulgazione arrechi, anche potenzialmente, un danno all'Ente;
- ricevere, inviare o inoltrare messaggi o file la cui natura sia contraria a norme di legge;
- rispondere a e-mail di provenienza dubbia;
- utilizzare account personali per attivita' aziendali e inviare messaggi file riguardanti l'attività lavorativa.

È vietata la navigazione in internet per motivi personali. L'ente ha adottato uno specifico sistema di blocco automatico che inibisce la navigazione in determinati siti inseriti in una black list.

È vietato l'uso dei social network per scopi personali. Solo il personale autorizzato dal proprio Responsabile

dell'area di appartenenza potrà utilizzare i social network e solo ed esclusivamente per ragioni lavorative.

L'utente è responsabile di ogni azione, dichiarazione, commento, pubblicazione effettuata mediante i social network anche qualora l'esternazione abbia ad oggetto o riguardi, anche indirettamente, la sua attività lavorativa e/o l'Ente o i suoi dipendenti.

L'utente a cui viene assegnato il PC portatile ha l'obbligo di custodirlo con diligenza e dovrà periodicamente collegarsi alla rete interna dell'Ente per consentire il caricamento dell'aggiornamento del software antivirus.

Non è consentito l'uso di abbonamenti privati per collegarsi alla rete.

L'utente a cui è affidato il telefono aziendale dovrà custodirlo con diligenza; ne è vietato l'uso per scopi personali salvo diversa determinazione della DG che potrà consentirne l'uso promiscuo. In caso di furto, smarrimento o danneggiamento, il dipendente dovrò darne comunicazione all'ente per consentire allo stesso di effettuare la disattivazione della scheda.

A seguito dell'emergenza sanitaria da Covid-19, sarà pertanto necessario rafforzare presidi di controllo specifici, eventualmente già adottati, volti al monitoraggio degli strumenti informatici dei lavoratori, il cui utilizzo oggi risulta fortemente incrementato, richiamando gli stessi al relativo corretto utilizzo in conformità con le procedure e le policy aziendali adottate.

GESTIONE ARCHIVI E DOCUMENTAZIONE

Il back – up dei dati avviene tramite 2 NAS supporti dischi Raid 5.

Pertanto, il back – up avviene: tutti i giorni parziale e settimanalmente totale.

La gestione dei supporti removibili del Consorzio è legata principalmente all'attività di trasferimento dei dati dall'esterno verso l'interno e trasferimento interno (tra gli apparati delle unità operative).

Se non espressamente autorizzati dalla DG e dal Responsabile dell'area informatica, non è consentito a terzi l'utilizzo di supporti removibili sugli apparati aziendali (PC, Notebook e Server).

GESTIONE FORNITORI DEI SERVIZI INFORMATICI

I Fornitori di Servizi Informatici dell'Ente dovranno condividere e sottoscrivere i principi generali di comportamento indicati nel Codice Etico e i protocolli di comportamento indicati nel presente Modello.

Ciascun contratto di consulenza e/o di fornitura di servizio e/o opere prevede clausole di riservatezza dei dati e di non divulgazione delle informazioni.

Il servizio di assistenza è garantito giornalmente e, previa richiesta del Consorzio, vengono eseguiti specifici interventi di assistenza e manutenzione della rete aziendale.

4.3. Responsabilità e gestione del protocollo

L'autorizzazione all'emissione e la diffusione del protocollo sono di competenza della DG.

Ogni modifica al presente protocollo deve essere approvata dalla DG e comunicata all'OdV che valuterà l'adeguatezza e la coerenza del Modello.

4.4. Diffusione del protocollo

Al fine di garantire l'efficacia del Modello, il Consorzio assicura l'ampia diffusione del protocollo e dei codici di comportamento di cui ai punti che precedono, mediante consegna *brevi manu* o diffusione via *e-mail*.

Tale protocollo rimane, in ogni caso, a disposizione presso gli Uffici amministrativi del Consorzio.